PURE STATES, NONNEGATIVE POLYNOMIALS AND SUMS OF SQUARES

SABINE BURGDORF, CLAUS SCHEIDERER, AND MARKUS SCHWEIGHOFER

Professor Alexander Prestel gewidmet aus Anlass seiner Emeritierung

Abstract. In recent years, much work has been devoted to a systematic study of polynomial identities certifying strict or non-strict positivity of a polynomial f on a basic closed set $K \subset \mathbb{R}^n$. The interest in such identities originates not least from their importance in polynomial optimization. The majority of the important results requires the archimedean condition, which implies that K has to be compact. This paper introduces the technique of pure states into commutative algebra. We show that this technique allows an approach to most of the recent archimedean Stellensätze that is considerably easier and more conceptual than the previous proofs. In particular, we reprove and strengthen some of the most important results from the last years. In addition, we establish several such results which are entirely new. They are the first that allow f to have arbitrary, not necessarily discrete, zeros in K.

Introduction

Consider a sequence $g_1, \ldots, g_r \in \mathbb{R}[\mathbf{x}] = \mathbb{R}[x_1, \ldots, x_n]$ of real polynomials together with the basic closed semi-algebraic set $K = \{x\colon g_1(x) \geq 0, \ldots, g_r(x) \geq 0\}$ in $\mathbb{R}^n$. Given a polynomial $f \in \mathbb{R}[\mathbf{x}]$ which is nonnegative on K, it is an important problem, both from a theoretical and from a practical point of view, to understand whether there exist simple algebraic certificates that make the nonnegative character of f evident. Traditionally, a result stating the existence of a particular type of such certificates is called a *Positivstellensatz*, or a *Nichtnegativstellensatz*, depending on whether f is supposed to be strictly or only non-strictly positive.

Krivine [Kr1] and Stengle [St] proved that such certificates always exist. However, their results amount to rational representations of f, that is, representations with denominators. Much harder to establish, but also much more powerful when they exist, are denominator-free representations of f,

Date: May 26, 2009.

2000 *Mathematics Subject Classification.* Primary 06F20, 11E25, 13J30; Secondary 06F25, 13A15, 14P10, 26C99, 46L30, 52A99.

Key words and phrases. pure states, extremal homomorphisms, order units, nonnegative polynomials, sums of squares, convex cones, quadratic modules, preorderings, semirings.

such as

$$f = s_0 + \sum_{i=1}^{r} s_i g_i, \quad f = \sum_{i_1=0}^{1} \cdots \sum_{i_r=0}^{1} s_{i_1,\ldots,i_r} \cdot g_1^{i_1} \cdots g_r^{i_r}$$

or

$$f = \sum_{i_1,\ldots,i_r \geq 0} a_{i_1,\ldots,i_r} \cdot g_1^{i_1} \cdots g_r^{i_r},$$

in which the s_i or $s_{i_1,\ldots,i_r}$ are sums of squares of polynomials and the $a_{i_1,\ldots,i_r}$ are nonnegative real numbers. The study of such identities comprises questions of existence and complexity as well as algorithmic aspects. Considerable research efforts have been spent in recent years on these questions (see [PD], [Ma2], [Sch4]), not least because of their central importance in polynomial optimization (see [La] for an excellent survey).

An *urversion* of a denominator-free representation result is the so-called archimedean representation theorem, due to Stone, Krivine, Kadison, Dubois and others. See [PD] Sect. 5.6, and also Thm. 6.1 below. It asserts that f has a representation as desired, provided that $f > 0$ on K and the archimedean condition holds. Many refinements of this result have been proved in the last decade, notably extensions to cases where f is allowed to have zeros in K. Some of them are recalled in Sect. 6 below. A common feature of all these results is the archimedean hypothesis. See 1.2 for its technical definition. Note that in any case, this condition implies that K is bounded, hence compact.

The purpose of this paper is to lay out a new approach to these results and to new archimedean *Stellensätze*, which is based on pure states of the associated cones in $\mathbb{R}[\mathtt{x}]$. This new approach permits proofs which are considerably more transparent, easy and uniform than the existing ones. In a number of cases, we arrive at substantially stronger results than known so far. In addition, using the new technique, we prove several archimedean Nichtnegativstellensätze which are completely new. Altogether, we believe that this paper gives ample support to our claim that the consequent use of pure states is a powerful tool in the study of archimedean Stellensätze. We remark that the results presented here do by far not exhaust the applications of this technique. We plan to give further applications elsewhere.

The technique of pure states relies on an old separation theorem for convex sets in a real vector space V, due to Eidelheit and Kakutani ([Ei], [Kk]). Combined with the Krein-Milman theorem, it yields a sufficient condition for membership in a convex cone $C \subset V$, provided that C has an order unit (also known as algebraic interior point): If $x \in V$ and all nonzero states of C have strictly positive value in x, then $x \in C$. The first systematic use of this criterion was probably made by Goodearl and Handelman [GH].

The starting point for this work was a remark of Handelman made to the third author in 2004. Handelman pointed out that a slightly weaker version of Theorem 2 in [Sw2] (corresponding to the special case $M = S$ in Theorem 6.4 below) can be proved easily by using pure states.

We now give a brief overview of the contents of this paper. Among its seven sections, the first five are preparatory in character, while the last two contain the main applications. After a few notational preliminaries in Sect. 1, we recall the general Goodearl-Handelman criterion in Sect. 2. From Sect. 3 on we work in a commutative ring A and consider (pseudo-) modules M over subsemirings S of A. After studying order units in such M in general (Sect. 3), we prove an important fact in Sect. 4, which applies in the situations which are most common (S archimedean or S containing all squares): If M contains an order unit with respect to the ideal it generates, then the associated pure states satisfy a multiplicative law of a very peculiar form. See Cor. 4.12 for a summarizing statement. This fact lies at the basis of all later applications. Sect. 5 discusses the question whether intersecting M with an ideal of A preserves the existence of an order unit. This is an important technical point, as explained in 3.8.

In Sect. 6 we review some of the most important Positiv- and Nichtnegativstellensätze in real algebra. Using pure states, we reprove them in an elegant and uniform way. For some of them we arrive at statements that are considerably stronger than previously known (Theorems 6.4, 6.5). Finally, in Sect. 7 we use pure states to arrive at Nichtnegativstellensätze which are entirely new. The so far known results of this type apply only (essentially) in the case where the zeros of the polynomial f in K are discrete. The two main results presented here are Theorems 7.6 and 7.11. In both, the zero set of f in K can have any dimension. While in Thm. 7.6, this zero set necessarily lies in the boundary of K (relative to its Zariski closure), Thm. 7.11 applies typically when the zeros lie in the (relative) interior of K. A particularly concrete case of Thm. 7.6 is Thm. 7.8, dealing with polynomials nonnegative on a polytope and vanishing on a face. It becomes visible in Theorems 7.6 and 7.11 how pure states on suitable ideals of the polynomial ring are closely related to directional derivatives (of order one in 7.6, of order two in 7.11).

In most parts of this paper, our setup is more general than real polynomial rings and semi-algebraic sets in $\mathbb{R}^n$. We explain in 1.6 why we think such a greater generality is necessary.

1. Notations and conventions

1.1. We start by recalling some terminology (mostly standard) from real algebra. General references are [PD], [Ma2], [Sch4].

Let A be a commutative ring (always with unit), and let $S \subset A$ be a semiring, i. e., a subset containing $\{0, 1\}$ and closed under addition and multiplication. A subset $M \subset A$ is called an *S-pseudomodule* if $0 \in M$, $M + M \subset M$ and $SM \subset M$. If in addition $1 \in M$ then M is said to be an *S-module*. The *support* of M is the subgroup $\mathrm{supp}(M) = M \cap (-M)$ of A; this is an ideal of A if $S - S = A$. We sometimes write $a \leq_M b$ to express that $b - a \in M$, for a, $b \in A$. The relation $\leq_M$ is anti-symmetric modulo

$\operatorname{supp}(M)$, transitive, and compatible with addition and with multiplication by elements of S.

Particularly important is the case where $S = \Sigma A^2$, the semiring of all sums of squares in A. The ΣA^2- (pseudo-) modules are called *quadratic (pseudo-) modules* in A. A semiring $S \subset A$ is called a *preordering* in A if it contains ΣA^2. When $\frac{1}{2} \in A$ we have $\Sigma A^2 - \Sigma A^2 = A$ by the identity $4x = (x+1)^2 - (x-1)^2$, and so, in this case, $\operatorname{supp}(M)$ is an ideal for every quadratic pseudomodule M.

Given finitely many elements $a_1, \ldots, a_r \in A$, we write

$$\operatorname{QM}(a_1, \ldots, a_r) \;:=\; \Sigma A^2 + \Sigma A^2 \cdot a_1 + \cdots + \Sigma A^2 \cdot a_r$$

resp.

$$\operatorname{PO}(a_1, \ldots, a_r) \;:=\; \operatorname{QM}\big(a_1^{i_1} \cdots a_r^{i_r} \colon i_1, \ldots, i_r \in \{0,1\}\big)$$

for the quadratic module (resp. the preordering) generated by $a_1, \ldots, a_r$ in A.

1.2. Let $M \subset A$ be an additive semigroup containing 1. Then M is said to be *archimedean* if for every $a \in A$ there is $n \in \mathbb{N}$ with $a \leq_M n$. In other words, M is archimedean if and only if $A = \mathbb{Z} + M$.

Note that when M is archimedean, every semigroup containing M is archimedean as well. See Remark 3.3 below for examples of archimedean semigroups.

Warning 1.3. In the functional analytic literature, M like in 1.2 is called archimedean if no $a \in A \setminus M$ has the property that $\mathbb{N}a$ has a lower bound in A with respect to $\leq_M$ (see, e. g., p. 20 in [Go]). Our definition is completely different and coincides with the usual terminology in real algebra (see, e. g., 1.5.1 in [Sch4]).

1.4. Given any subset $M \subset A$, we write

$$X(M) := \big\{\phi \in \operatorname{Hom}(A, \mathbb{R}) \colon \phi|_M \geq 0\big\}$$

(where $\operatorname{Hom}(A, \mathbb{R})$ denotes the set of ring homomorphisms $A \to \mathbb{R}$) and

$$Z(M) := X(M \cup -M) = \big\{\phi \in \operatorname{Hom}(A, \mathbb{R}) \colon \phi|_M = 0\big\}.$$

Considering $\operatorname{Hom}(A, \mathbb{R})$ as a subset of $\mathbb{R}^A = \prod_A \mathbb{R}$, this set has a natural topology. When M is an archimedean semigroup in A, the subset $X(M)$ of $\operatorname{Hom}(A, \mathbb{R})$ is compact.

Write $X := \operatorname{Hom}(A, \mathbb{R})$. Every $a \in A$ induces a continuous map $\widehat{a} \colon X \to \mathbb{R}$ by evaluation. Thus we have the canonical ring homomorphism (not necessarily injective)

$$A \to C(X, \mathbb{R}), \quad a \mapsto \widehat{a}$$

(here $C(X, \mathbb{R})$ is the ring of continuous real-valued functions on X). Thinking in this way of the elements of A as $\mathbb{R}$-valued functions, it is natural to write $a(x)$ instead of $x(a)$, for $a \in A$ and $x \in X$, an abuse of notation that we will often commit.

Scholium 1.5. Let A be a finitely generated $\mathbb{R}$-algebra. To emphasize the geometric point of view we will frequently identify $\mathrm{Hom}(A,\mathbb{R})$ with $V(\mathbb{R})$, the set of $\mathbb{R}$-points of the affine algebraic $\mathbb{R}$-scheme $V = \mathrm{Spec}(A)$. Thus, if $M \subset A$ is any subset, we have

$$X(M) = \{x \in V(\mathbb{R})\colon \forall\, f \in M\ f(x) \geq 0\}.$$

If M is finite, or a finitely generated quadratic module in A, $X(M)$ is a basic closed semi-algebraic set in $V(\mathbb{R})$.

Any choice of finitely many $\mathbb{R}$-algebra generators $a_1, \ldots, a_n$ of A gives an identification of $\mathrm{Hom}(A,\mathbb{R}) = V(\mathbb{R})$ with a real algebraic subset of $\mathbb{R}^n$, via the map

$$\mathrm{Hom}(A,\mathbb{R}) \hookrightarrow \mathbb{R}^n, \quad x \mapsto \big(x(a_1), \ldots, x(a_n)\big).$$

The image set is the zero set of the ideal of relations between $a_1, \ldots, a_n$, and hence is real algebraic. Generally it is preferable not to fix a set of generators in advance, and only to introduce affine coordinates when it becomes necessary.

1.6. A word on the generality of our setup. Preorderings, and more generally quadratic modules, in polynomial rings over $\mathbb{R}$ are the most traditional context for positivity results (see [PD], [Ma2], [Sch4]). But there are also prominent examples which do not fit this context, like theorems by Pólya and Handelman [H1], [H2], [Sw2]. These are cases where the required algebraic objects are semirings, or modules over semirings. It is often preferable, or even necessary, to work with arbitrary finitely generated $\mathbb{R}$-algebras, instead of just polynomial rings over $\mathbb{R}$. Finally, we feel that applications to rings of arithmetic nature, like finitely generated algebras over $\mathbb{Z}$ or $\mathbb{Q}$, are interesting enough as to not exclude these cases a priori.

Given all this, our basic general setup will consist of a ring A and an additive semigroup $M \subset A$ (with $0 \in M$). We feel free to assume $\mathbb{Q} \subset A$ and $\mathbb{Q}_+M \subset M$ when this helps to simplify technical details. Usually this does not mean much loss of generality, since one can always pass from A and M to $A_{\mathbb{Q}} = A \otimes \mathbb{Q}$ and $M_{\mathbb{Q}} = \{x \otimes \frac{1}{n}\colon n \in \mathbb{N}\}$. None of the methods discussed in this paper sees a difference between $f \in M$ and $\exists\, n \in \mathbb{N}\ nf \in M$.

1.7. By $\mathbb{N} = \{1, 2, 3, \ldots\}$ we denote the set of natural numbers. The set of nonnegative rational, resp. nonnegative real, numbers is written $\mathbb{Q}_+$, resp. $\mathbb{R}_+$.

2. Convex cones and pure states

2.1. Let G be an abelian group, written additively, and let $M \subset G$ be a subsemigroup (always containing 0). The subgroup $\mathrm{supp}(M) := M \cap (-M)$ of G is called the *support* of M. We neither assume $\mathrm{supp}(M) = \{0\}$ nor $M - M = G$ in general. It is often useful to work with the relation $\leq_M$ on G defined by $x \leq_M y :\Leftrightarrow y - x \in M$.

A group homomorphism $\varphi\colon G \to \mathbb{R}$ into the additive group of reals is called a *state* of (G, M) if $\varphi|_M \geq 0$. We sometimes denote the convex cone of all states by $S(G, M)$.

An element $u \in M$ is called an *order unit* of (G, M) if $G = M + \mathbb{Z}u$, or equivalently, if for every $x \in G$ there is $n \in \mathbb{N}$ with $x \leq_M nu$. In general, there need not exist any order unit, not even when $G = M - M$ (which clearly is a necessary condition).

Example 2.2. If A is a ring and $M \subset A$ is an additive semigroup containing 1, then M is archimedean (see 1.2) if and only if 1 is an order unit of (A, M).

Example 2.3. A typical and frequently used example is when $G = V$ is a vector space over $\mathbb{R}$ (of any dimension) and M is a *convex cone* in V, i. e., M is non-empty and satisfies $M + M \subset M$ and $\mathbb{R}_+ M \subset M$. The convex cone $S(V, M)$ of all states of (V, M) is equal to the *dual cone*

$$M^* \;=\; \big\{\varphi \in V^\vee \colon \varphi|_M \geq 0\big\}$$

of M (regarded as sitting in the dual linear space $V^\vee$), provided that $V = M - M$. (If M does not span V, there exist additive maps $V \to \mathbb{R}$ vanishing on M which are not $\mathbb{R}$-linear.)

The order units of (V, M) are also known under the name *algebraic interior points* of M (e. g. [Kö] p. 177, [Ba] III.1.6). In particular, when $\dim(V) < \infty$, the order units of (V, M) are precisely the interior points of M with respect to the euclidean topology on V. Hence, in this case, an order unit exists if and only if $V = M - M$.

2.4. Assume that (G, M) has an order unit u. Then every nonzero state φ of (G, M) satisfies $\varphi(u) > 0$. We say that φ is a *monic state* of (G, M, u), or for brevity, simply a *state* of (G, M, u), if $\varphi(u) = 1$. The set of all monic states will be denoted $S(G, M, u)$.

The set $S(G, M, u)$ can be regarded as a subset of the product vector space $\mathbb{R}^G = \prod_G \mathbb{R}$. As such it is compact and convex. A state $\varphi \in S(G, M, u)$ is called a *pure state* of (G, M, u) if it is an extremal point of the compact convex set $S(G, M, u)$, or equivalently, if $2\varphi = \varphi_1 + \varphi_2$ with $\varphi_1,\ \varphi_2 \in S(G, M, u)$ implies $\varphi = \varphi_1 = \varphi_2$.

By the Krein-Milman theorem, the convex hull of the set of pure states of (G, M, u) is dense in $S(G, M, u)$. Using this fact together with the Eidelheit-Kakutani separation theorem ([Ei], [Kk], see also [Ba] III.1.7), one can prove the following fundamental result. Originally it is due to Effros, Handelman and Shen [EHS] (see also Lemma 4.1 in [GH] and Theorem 4.12 in [Go]).

Theorem 2.5. *Let G be an abelian group and $M \subset G$ a semigroup in G with order unit u. Let $x \in G$. If $\varphi(x) > 0$ for every pure state φ of (G, M, u), there is an integer $n \geq 1$ with $nx \in M$.* □

Remarks 2.6. Let G be an abelian group and $M \subset G$ a semigroup.

1. Let $G_{\mathbb{Q}} = G \otimes \mathbb{Q}$ and $M_{\mathbb{Q}} = \{x \otimes q \colon x \in M,\, q \in \mathbb{Q}_+\}$. Then $S(G,M) = S(G_{\mathbb{Q}}, M_{\mathbb{Q}})$ holds canonically. If $u \in M$ is an order unit of (G,M) then $u \otimes 1$ is an order unit of $(G_{\mathbb{Q}},\, M_{\mathbb{Q}})$ (the converse being false in general), and we have $S(G,M,u) = S(G_{\mathbb{Q}}, M_{\mathbb{Q}}, u \otimes 1)$. In this way one reduces the proof of Theorem 2.5 to the case where G is a $\mathbb{Q}$-vector space and $\mathbb{Q}_+ M = M$.

2. In the situation of Theorem 2.5, $\varphi(x) > 0$ holds for every pure state of (G,M,u) if and only if $\varphi(x) > 0$ holds for every $0 \neq \varphi \in S(G,M)$. Therefore, the condition on x in 2.5 is independent of the choice of a particular order unit. As for the claim, note that the map $S(G,M,u) \to \mathbb{R}$, $\varphi \mapsto \varphi(x)$ assumes its minimum since $S(G,M,u)$ is compact. The set of minimizers is compact and convex, and hence has an extremal point φ. One verifies that any such φ is also an extremal point of $S(G,M,u)$, i. e., a pure state of (G,M,u).

Corollary 2.7. *Assume that (G,M) has an order unit u, and that M satisfies ($na \in M \Rightarrow a \in M$) for every $a \in G$ and $n \in \mathbb{N}$. Let $x \in G$ with $\varphi(x) > 0$ for every pure state φ of (G,M,u). Then x is an order unit of (G,M).*

Proof. $x \in M$ by a direct application of Theorem 2.5, using the assumption on M. Given $y \in G$, the map $\varphi \mapsto \frac{\varphi(y)}{\varphi(x)}$ from the (compact convex) set $S(G,M,u)$ to $\mathbb{R}$ is continuous. Hence there is $n \in \mathbb{N}$ with $\left|\frac{\varphi(y)}{\varphi(x)}\right| < n$, i. e., $\varphi(nx \pm y) > 0$, for every $\varphi \in S(G,M,u)$. Again from 2.5 and the assumption we get $nx \pm y \in M$. □

3. Order units in rings and ideals

Definition 3.1. Let A be a ring and $M \subset A$ an additive semigroup (with $0 \in M$, as always). For $u \in M$ we put

$$O(M,u) := O_A(M,u) := \big\{a \in A \colon \exists\, n \in \mathbb{N}\ nu \pm a \in M\big\},$$

or equivalently, $O(M,u) = \operatorname{supp}(M + \mathbb{Z}u)$.

So $O(M,u)$ consists of all elements which are bounded "in absolute value" by some positive multiple of u, with respect to $\leq_M$.

Proposition 3.2. *Let M, M_1, M_2 be additive semigroups in A.*

(a) *Let $u \in M$. Then $O(M,u)$ is an additive subgroup of $M - M \subset A$ containing* $\operatorname{supp}(M) + \mathbb{Z}u$.

(b) *$O(M_1,u_1) \cdot O(M_2,u_2) \subset O(M_1M_2, u_1u_2)$ for all $u_1 \in M_1$, $u_2 \in M_2$, where M_1M_2 denotes the semigroup in A generated by all products x_1x_2 with $x_i \in M_i$ ($i = 1,2$).*

(c) *Let S be a semiring in A. Then $O(S,1)$ is a subring of A, and $O(S,u)$ is an $O(S,1)$-submodule of A for every $u \in S$.*

(d) *Assume that $\frac{1}{2} \in A$ and M is a quadratic module. Then $O(M,1)$ is a subring of A, and $O(M,u)$ is an $O(M,1)$-submodule of A for every $u \in M$ with $uM \subset M$.*

Proof. (a) is obvious. For the proof of (b) let $a_i \in O(M_i, u_i)$, say $n_i u_i \pm a_i \in M_i$ with $n_i \in \mathbb{N}$ $(i = 1, 2)$. From

$$\begin{aligned} 3n_1n_2\, u_1u_2 + \varepsilon a_1a_2 &= (n_1u_1 + a_1)(n_2u_2 + \varepsilon a_2) \\ &\quad + n_1u_1(n_2u_2 - \varepsilon a_2) + n_2u_2(n_1u_1 - a_1) \end{aligned}$$

for $\varepsilon = \pm 1$ we see $a_1a_2 \in O(M_1M_2, u_1u_2)$.

(c) is an immediate consequence of (b). To prove (d) let $a \in O(M, 1)$, say $m \pm a \in M$. If $r > \frac{m}{2}$ is an integer, the identity

$$(r - a)^2(m + a) + (r + a)^2(m - a) = 2r^2m - 2(2r - m)a^2$$

shows $a^2 \in O(M, 1)$. Given another element $b \in O(M, 1)$, we get $ab \in O(M, 1)$ from $4ab = (a + b)^2 - (a - b)^2$. So $O(M, 1)$ is a subring of A.

Now let $u \in M$ with $uM \subset M$, let $x \in O(M, u)$ and let $a \in O(M, 1)$ be as before. We have $nu \pm x \in M$ for some $n \in \mathbb{N}$, i. e. $\pm x \leq_M nu$. Multiplying with a^2 gives $\pm a^2x \leq_M na^2u$. By what was said before there is $k \in \mathbb{N}$ with $a^2 \leq_M k$. Using $uM \subset M$ we conclude $a^2u \leq_M ku$, and therefore $\pm a^2x \leq_M nku$. This shows $a^2 \cdot O(M, u) \subset O(M, u)$ for every $a \in O(M, 1)$, and $O(M, u)$ is an $O(M, 1)$-submodule of A. □

Remarks 3.3.

1. If $M \subset A$ is a semigroup containing 1, then M is archimedean (1.2) if and only if $O(M, 1) = A$.

2. More generally, let $M \subset A$ be any semigroup and $u \in M$. Then $O(M, u)$ is the largest subgroup B of A containing u with the property that u is an order unit of $(B, M \cap B)$.

3. The rings $O(M, 1)$ were introduced in [Sw1], in the case where M is a preordering. The fundamental result proved in [Sw1] is that when A is an $\mathbb{R}$-algebra of finite transcendence degree d and $T \subset A$ is a preordering, then $O(T, 1)$ coincides with $H^d(A, T)$, the d times iterated ring of geometrically bounded elements. (See *loc. cit.* for precise details.)

4. A special case of the just mentioned result is the celebrated theorem of Schmüdgen [Sm]: If A is a finitely generated $\mathbb{R}$-algebra and $T \subset A$ is a finitely generated preordering, then T is archimedean if (and only if) the basic closed set $X(T)$ is compact.

5. The article [JP] (see also [PD] and [Ma2]) is concerned with the question when quadratic modules are archimedean. In general, this is much more subtle than for preorderings.

6. Let $K \subset \mathbb{R}^n$ be a nonempty compact convex polyhedron, described by linear inequalities $g_1 \geq 0, \ldots, g_s \geq 0$. Let S be the semiring generated in the polynomial ring $\mathbb{R}[\mathbf{x}] := \mathbb{R}[x_1, \ldots, x_n]$ by $\mathbb{R}_+$ and $g_1, \ldots, g_s$. By a classical theorem of Minkowski (Thm. 5.4.5 in [PD]), the cone $\mathbb{R}_+ + \mathbb{R}_+g_1 + \cdots + \mathbb{R}_+g_s \subset S$ contains every linear polynomial which is nonnegative on K. Using compactness of K it follows that $O(S, 1)$ contains all linear polynomials. Since $O(S, 1)$ is a subring of $\mathbb{R}[\mathbf{x}]$ (3.2(c)), it follows that S is archimedean.

Corollary 3.4. *Let $S \subset A$ be a semiring and $M \subset A$ an S-module. Let I, J be ideals of A such that $(I, S \cap I)$ has an order unit u and $(J, M \cap J)$ has an order unit v. Then uv is an order unit of $(IJ,\ M \cap IJ)$.*

Proof. The hypotheses say $I \subset O(S, u)$ and $J \subset O(M, v)$. By 3.2(b) we have $IJ \subset O(M, uv)$, which is precisely what was claimed. □

Proposition 3.5. *Assume that M is a pseudomodule over an archimedean semiring S in A. Then*

$$O(M, f) \;=\; \mathrm{supp}(M + Af)$$

for every $f \in M$, and this is an ideal of A.

Proof. $\mathrm{supp}(M + Af)$ is an ideal since it is stable under multiplication with S and since $S + \mathbb{Z} = A$. The inclusion $O(M, f) = \mathrm{supp}(M + \mathbb{Z}f) \subset \mathrm{supp}(M + Af)$ is clear. Conversely let $g \in \mathrm{supp}(M + Af)$, say $g = x + af = -y + bf$ with $x, y \in M$ and $a,\ b \in A$. Since S is archimedean, there is $n \in \mathbb{N}$ with $n \pm a \in S$ and $n \pm b \in S$. Therefore $nf - g = (n - b)f + y$ and $nf + g = (n + a)f + x$ lie in M, which shows $g \in O(M, f)$. □

Here is an equivalent formulation:

Corollary 3.6. *Let M be a pseudomodule over an archimedean semiring in A, and let $f \in M$. Then f is an order unit of $(I, M \cap I)$ where $I := \mathrm{supp}(M + Af)$ (an ideal of A).*

Proof. The inclusion $I \subset O(M, f)$, which holds by 3.5, means that f is an order unit of $(I, M \cap I)$ (see 3.3). □

Using the Goodearl-Handelman criterion, we can give still another formulation:

Corollary 3.7. *Assume $\mathbb{Q} \subset A$. Let S be an archimedean semiring in A with $\mathbb{Q}_+ \subset S$, let M be a pseudomodule over S, and let $f \in A$ be fixed. Then $f \in M$ if and only if there exists an ideal $I \subset A$ with $f \in I$ having the following two properties:*

(1) *$(I, M \cap I)$ has an order unit u;*
(2) *$\varphi(f) > 0$ for every pure state φ of $(I, M \cap I, u)$.*

Moreover, when $f \in M$, the ideals I with the above properties are precisely the ideals satisfying $Af \subset I \subset \mathrm{supp}(M + Af)$.

Proof. If I is an ideal containing f with (1) and (2), then we get $f \in M$ directly using 2.5. Conversely assume $f \in M$. Then $I := \mathrm{supp}(M + Af)$ has the desired properties. Indeed, f itself is an order unit of $(I, M \cap I)$ (3.6). The last assertion in 3.7 is also contained in 3.6, cf. the remark in 3.3. □

Remark 3.8. Suppose we have A, S and M as before, and are given an element $f \in A$ of which we want to prove that it lies in M. Corollary 3.7 shows a possible way to proceed. In fact, most of the main results of this paper will be concretizations of this corollary in one or the other way. At

this point, we would like to point out the need of understanding the following two questions:

(Q1) Given an archimedean S-module M and an ideal I of A, when does $(I, M \cap I)$ have an order unit u?

(Q2) If u is such an order unit, what are the pure states of $(I, M \cap I, u)$?

We will address (Q1) in Sect. 4 and (Q2) in Sect. 5.

Remark 3.9. Without the archimedean condition on S, a result like 3.6 is usually far from true. This is demonstrated by the following example: Let $M = \mathrm{QM}(x,\, y,\, 1-x-y)$ in $A = \mathbb{R}[x, y]$, an archimedean quadratic module by Proposition 3.2(d), and consider the element $f = x$ of M. Then $\mathrm{supp}(M + Ax) = Ax =: I$, but x is not an order unit of $(I, M \cap I)$ (or equivalently, $O(M, x)$ is strictly smaller than I). For example, $cx \pm xy \notin M$ for any $c \in \mathbb{R}$, as is easily seen. In fact, we will show in 5.7 below that $(I, M \cap I)$ does not have any order unit at all.

4. Pure states on rings and ideals

In 3.8 we have seen why it is important to have a good understanding of the pure states of (I, M, u), where I is an ideal of A and $M \subset I$ is an S-pseudomodule over S with order unit u. We shall now give a satisfactory characterization in two important cases, namely when S is archimedean, or when M is archimedean and $S = \Sigma A^2$. These results are variations of a theorem by Handelman ([H1], Prop. 1.2). The main idea partially appears to some extent already in earlier work, see Thm. 10 in [BLP] or Thm. 15 in [Kr1].

Proposition 4.1. *Let A be a ring and $I \subset A$ an ideal. Let $S \subset A$ be an archimedean semiring and $M \subset I$ an S-pseudomodule, and assume that (I, M) has an order unit u. Then every pure state φ of (I, M, u) satisfies the following multiplicative law:*

$$\forall\, a \in A\ \forall\, b \in I \quad \varphi(ab) = \varphi(au) \cdot \varphi(b). \tag{1}$$

4.2. Before we start the proof of 4.1, here are some preparations. Let u be an order unit of (I, M). Given an additive map $\varphi\colon I \to \mathbb{R}$, and given any $a \in A$ with $\varphi(au) \neq 0$, let $\varphi_a\colon I \to \mathbb{R}$ be the *localization* of φ by a, defined by

$$\varphi_a(b) \;:=\; \frac{\varphi(ab)}{\varphi(au)} \quad (b \in I).$$

Clearly, φ_a is an additive map with $\varphi_a(u) = 1$. If φ is a state of (I, M) and $aM \subset M$, then φ_a is a state of (I, M, u). If $a_1,\, a_2 \in A$ satisfy $\varphi(a_i u) > 0$ $(i = 1, 2)$ then

$$\varphi(a_1 u) \cdot \varphi_{a_1} + \varphi(a_2 u) \cdot \varphi_{a_2} = \varphi((a_1 + a_2)u) \cdot \varphi_{a_1 + a_2},$$

so $\varphi_{a_1+a_2}$ is a proper convex combination of φ_{a_1} and φ_{a_2} in this case.

4.3. *Proof of Proposition 4.1*: In proving (1) we can assume $a \in S$ since $A = S + \mathbb{Z}$. Fixing $a \in S$ there are two cases:

If $\varphi(au) = 0$, we have to show $\varphi(aI) = 0$. Now $aI = aM + \mathbb{Z}au$, and so it is enough to prove $\varphi(aM) = 0$. For any $x \in M$ there is $n \in \mathbb{N}$ with $0 \leq_M x \leq_M nu$, whence $0 \leq_M ax \leq_M nau$, from which we get $\varphi(ax) = 0$.

There remains the case where $\varphi(au) > 0$. Since S is archimedean there is $n \in \mathbb{Z}$ with $a \leq_S n$. Choosing n so large that $\varphi(au) < n = \varphi(nu)$, we can consider the localized (monic) states φ_a and φ_{n-a}. As remarked before, $\varphi_n = \varphi$ is a proper convex combination of the two. Since φ is a pure state we must have $\varphi_a = \varphi$, which is identity (1). □

The case $I = A$ and $u = 1$ deserves special attention:

Corollary 4.4. *Let M be a module over an archimedean semiring in A. Then every pure state of $(A, M, 1)$ is a ring homomorphism $A \to \mathbb{R}$.* □

A result similar to 4.1 is also true for quadratic pseudomodules:

Theorem 4.5. *Let I be an ideal of A and $M \subset I$ a quadratic pseudomodule with order unit u of (I, M). Every pure state φ of (I, M, u) satisfies* (1) *of 4.1.*

The proof of 4.5 is somewhat more tricky. We need two auxiliary lemmas:

Lemma 4.6. *For $n \in \mathbb{N}$ let*

$$t_n(x) = \sum_{k=0}^{n} \binom{1/2}{k} (-x)^k,$$

the n-th Taylor polynomial of $\sqrt{1-x}$. Then the polynomial $t_n(x)^2 - (1-x)$ has nonnegative coefficients in $\mathbb{Z}\left[\frac{1}{2}\right]$.

Proof. Fix n, and write $p_n(x) := t_n(x)^2 - (1-x) =: \sum_{k \geq 0} c_k x^k$. Then $c_k = 0$ for $k \leq n$ or $k > 2n$, while

$$c_k = (-1)^k \sum_{i=k-n}^{n} \binom{1/2}{i} \binom{1/2}{k-i}$$

for $n < k \leq 2n$. The term with index i in the sum has sign $(-1)^{i-1} \cdot (-1)^{k-i-1} = (-1)^k$. This implies the lemma. □

Lemma 4.7. *Keep the assumptions of 4.5, assume moreover $\frac{1}{2} \in A$, and let $a \in A$ satisfy $aM \subset M$ and $(1-2a)u \in M$. Then every state φ of (I, M) satisfies $\varphi((1-a)M) \geq 0$.*

Proof. Normalizing φ we can assume that φ is monic, i. e., $\varphi(u) = 1$. By hypothesis we have $au \leq_M \frac{u}{2}$, and inductively we get $a^k u \leq_M 2^{-k} u$ for all $k \geq 0$. Let $b \in M$. There is $r \geq 0$ with $2^r u - b \in M$. In order to show $\varphi((1-a)b) \geq 0$ we may replace b by $2^{-r}b$, and may therefore assume $u - b \in M$. We will show $\varphi((1-a)b) > -\varepsilon$ for every real number $\varepsilon > 0$.

Let $t_n(x)$ be the Taylor polynomial from Lemma 4.6, and write $p_n(x) = t_n(x)^2 - (1-x)$. Due to the convergence of the binomial series, there is $n \in \mathbb{N}$ with $p_n(\frac{1}{2}) < \varepsilon$. Fix n and write $p := p_n$. According to 4.6 we have

$$p(x) = \sum_k c_k x^k$$

with nonnegative numbers $c_k \in \mathbb{Z}\big[\frac{1}{2}\big]$. So $aM \subset M$ implies $p(a)M \subset M$, and from $b \leq_M u$ we conclude $p(a)b \leq_M p(a)u$. In particular, $\varphi(p(a)b) \leq \varphi(p(a)u)$. On the other hand,

$$\varphi\big(p(a)u\big) = \sum_k c_k\, \varphi(a^k u) \;\leq\; \sum_k c_k 2^{-k} = p\Big(\frac{1}{2}\Big) \;<\; \varepsilon.$$

We conclude

$$\varphi\big(t_n(a)^2 b\big) - \varphi\big((1-a)b\big) = \varphi(p(a)b) \;\leq\; \varphi(p(a)u) \;<\; \varepsilon,$$

and so

$$\varphi\big((1-a)b\big) \;>\; \varphi(t_n(a)^2 b) - \varepsilon \;\geq\; -\varepsilon$$

since M is a quadratic pseudomodule. □

4.8. *Proof of Theorem 4.5:* We may pass from A, I and M to $A \otimes \mathbb{Q}$, $I \otimes \mathbb{Q}$ and $M_{\mathbb{Q}} = \{x \otimes \frac{1}{n} \colon x \in M,\, n \in \mathbb{N}\}$, respectively (see the remark in 2.6). In particular, we may assume $\frac{1}{2} \in A$, and thus have $\Sigma A^2 - \Sigma A^2 = A$. Therefore it is enough to prove identity (1) for $a \in \Sigma A^2$ and $b \in I$.

If $\varphi(au) = 0$, one shows $\varphi(aI) = 0$ as in 4.3. If $\varphi(au) > 0$, choose $k \in \mathbb{N}$ with $au \leq_M 2^k u$. For the proof of (1) we may replace a with $2^{-(k+1)}a$, and can thus assume $(1-2a)u \in M$. Lemma 4.7 now shows $\varphi((1-a)M) \geq 0$. As in the proof of 4.1, this makes φ a proper convex combination of the monic states φ_a and φ_{1-a}. Since φ is a pure state we conclude $\varphi = \varphi_a$, which is the assertion of 4.5. □

The algebraic meaning of identity 4.1 (1) is explained in the following easy lemma:

Lemma 4.9. *Let A be a ring, $I \subset A$ an ideal and $u \in I$. Let k be a field and $\varphi \colon I \to k$ an additive map satisfying $\varphi(u) = 1$. Equivalent conditions:*

(i) $\forall\, a \in A\ \forall\, b \in I\ \ \varphi(ab) = \varphi(au) \cdot \varphi(b)$*;*
(ii) *there is a ring homomorphism $\phi \colon A \to k$ such that $\varphi(ab) = \phi(a) \cdot \varphi(b)$ for $a \in A$, $b \in I$.*

Moreover, the homomorphism ϕ in (ii) is uniquely determined and satisfies $\phi(a) = \varphi(au)$ for $a \in A$. Exactly one of the following two alternatives holds:

(1) $\phi(u) \neq 0$ *and* $\varphi(b) = \frac{\phi(b)}{\phi(u)}$ *for every $b \in I$;*
(2) $\phi(I) = 0$.

Note that the alternatives (1), resp. (2), are equivalent to $\varphi(u^2) \neq 0$, resp. $\varphi(u^2) = 0$.

Proof. (i) $\Rightarrow$ (ii) One sees immediately that ϕ must satisfy $\phi(a) = \varphi(au)$ ($a \in A$). It is readily checked that the so-defined ϕ satisfies (ii). The converse is clear as well. Assuming that ϕ satisfies (ii), we have $\phi(b) = \phi(u) \cdot \varphi(b)$ for every $b \in I$. If $\phi(u) \neq 0$ then (1) holds. Otherwise $\phi(u) = 0$, and so $\phi(I) = 0$. □

Definition 4.10. In the situation of 4.9 we call ϕ the ring homomorphism *associated with* φ. We refer to the identity $\varphi(ab) = \phi(a)\varphi(b)$ (for $a \in A$, $b \in I$) by saying that φ is *ϕ-linear*.

The setting described in 4.9 is relevant to us since it arises from pure states in ideals, see 4.1 and 4.5. In this situation the following additional observation is important:

Lemma 4.11. *Let A be a ring, $I \subset A$ an ideal and $M \subset I$ an additive semigroup. Let $u \in M$, and let $\varphi\colon I \to \mathbb{R}$ be a state of (I, M, u) fulfilling* (1)*. Then the associated ring homomorphism $\phi\colon A \to \mathbb{R}$ satisfies $\phi \in X(T)$ where*

$$T := \{t \in A\colon tu \in M\}.$$

In particular, if $uM \subset M$ then $\phi \in X(M)$.

Proof. If $t \in A$ is such that $tu \in M$, then $\phi(t) = \varphi(tu) \geq 0$. □

Corollary 4.12 (Dichotomy)**.** *Let S be a semiring and I an ideal in A, and let $M \subset I$ be an S-pseudomodule such that (I, M) has an order unit u. Assume that S is either archimedean or a preordering. Given any pure state $\varphi\colon I \to \mathbb{R}$ of (I, M, u), precisely one of the following two statements is true:*

(I) *φ is a scaled ring homomorphism: There exists $\phi \in X(S)$ with $\phi(u) \neq 0$ such that $\varphi = \frac{1}{\phi(u)} \cdot \phi|_I$.*

(II) *There exists $\phi \in X(S + I)$ such that φ is ϕ-linear.*

More precisely, (I) $\Leftrightarrow \varphi(u^2) \neq 0$*, and* (II) $\Leftrightarrow \varphi(u^2) = 0$*. In both cases, ϕ is uniquely determined. In* (I) *(resp.* (II)*), one even has $\phi \in X(T)$ (resp. $\phi \in X(T + I)$) with T defined as in Lemma 4.11. Case* (II) *can occur only when $I \neq A$.*

Proof. This is Prop. 4.1 (for S archimedean) resp. Thm. 4.5 (for $\Sigma A^2 \subset S$), combined with 4.9. In both cases (I) and (II), note that ϕ is necessarily the ring homomorphism associated with φ (Def. 4.10), and hence is uniquely determined by φ. So the additional information $\phi \in X(T)$ follows from Lemma 4.11. □

Depending on u, the semiring T can be larger than S. This is sometimes useful, for example, in the proof of Thm. 6.4 below.

Remark 4.13. In general, both $\phi(u) > 0$ and $\phi(u) < 0$ are possible in case (I), and accordingly, both $\phi \in X(M)$ and $\phi \in X(-M)$. In many standard situations, however, the second cannot occur. For example, when $M = N \cap I$ for some quadratic module N of A, then necessarily $\phi \in X(M)$ since $u^2 \in M$. The same reasoning applies when M is a semiring.

Corollary 4.14. *Assume $\mathbb{Q} \subset A$, and let M be a quadratic module in A. If (A, M) has an order unit then M is archimedean.*

In other words, if (A, M) has an order unit, then 1 is such an order unit as well.

Proof. Let u be an order unit of (A, M). By 2.7 it suffices to show $\varphi(1) > 0$ for every pure state φ of (A, M, u). By 4.12, such φ satisfies $\varphi(b) = \frac{\phi(b)}{\phi(u)}$ $(b \in A)$ for some ring homomorphism $\phi\colon A \to \mathbb{R}$ with $\phi(u) \neq 0$. So $\varphi(1) = \frac{1}{\phi(u)} \neq 0$, and $1 \in M$ implies $\varphi(1) > 0$. □

Remark 4.15. It is natural to wonder where there is a converse to Corollary 4.12, in the following sense. In the situation given there, assume that φ is a state of (I, M, u) that satisfies the multiplicativity law (1) (and hence satisfies (I) or (II) of 4.12, by Lemma 4.9). Does it follow that φ is a pure state, i. e. is extremal in $S(I, M, u)$?

It is easy to see that the answer must be no in general, at least when φ is of type (II): Fixing ϕ, the ϕ-linear states of (I, M, u) usually form a convex (compact) set of positive dimension, so most of its elements are not extremal. For example, when $M = \mathrm{PO}(x,\, y,\, 1 - x - y)$ in $A = \mathbb{R}[x, y]$ and $I = (x, y)$ is the maximal ideal of the origin in A, then $u = x + y$ is an order unit of $(I, M \cap I)$ (this is shown in 5.1 below). The states of type (II) are the partial derivatives whose direction lies in the closed first quadrant (up to normalization). Hence only two of them are pure states.

However, when φ is of type (I), then under suitable additional side conditions on M it is indeed true that φ is necessarily pure. For example, this is so when $M = N \cap I$ for some quadratic module N in A:

Proposition 4.16. *Suppose $\mathbb{R} \subset A$. Let I be an ideal of A and $M \subset I$ a quadratic pseudomodule with $I = M - M$. We assume $a^2 \in M$ for every $a \in I$. Then every multiplicative state $\varphi \in S(I, M)$ is extremal in the cone $S(I, M)$, i. e., $\varphi = \varphi_1 + \varphi_2$ with $\varphi_i \in S(I, M)$ implies $\varphi_i = c_i\varphi$ with $c_i \geq 0$.*

By saying that φ is multiplicative, we mean here that $\varphi(xy) = \varphi(x)\varphi(y)$ holds for all $x, y \in M$.

When A is a ring (possibly without unit) of $\mathbb{R}$-valued functions on a set, the analogous result for multiplicative states of (A, A_+) was proved by Bonsall, Lindenstrauss and Phelps in 1966 ([BLP], Thm. 13). The same proof applies, essentially literally, in our situation as well. Since Prop. 4.16 and Cor. 4.17 won't be used elsewhere in this paper, we skip over the details. □

Combining Prop. 4.16 with Thm. 4.5 we conclude:

Corollary 4.17. *Suppose $\mathbb{R} \subset A$. Assume that M is an archimedean quadratic module in A. Then the pure states of $(A, M, 1)$ are precisely the elements of $X(M)$.* □

5. Existence of order units in ideals

Given an archimedean S-module M in A, and given an ideal I of A, we are going to study when the cutted-down pseudomodule $M \cap I$ has an order unit in I. See 3.8 for why this is an important question.

Proposition 5.1. *Let $S \subset A$ be a semiring and $M \subset A$ an S-pseudomodule, and let $I \subset A$ be an ideal generated by $x_1, \ldots, x_n$. Assume that one of the following two conditions holds:*

(1) *(A, S) has an order unit u, and $x_1, \ldots, x_n \in M$;*
(2) *(A, M) has an order unit u, and $x_1, \ldots, x_n \in S$.*

Then $v := u(x_1 + \cdots + x_n)$ is an order unit of $(I, M \cap I)$.

Proof. Any $b \in I$ can be written $b = \sum_{i=1}^n a_i x_i$ with $a_i \in A$ $(i = 1, \ldots, n)$. By assumption there is $k \in \mathbb{N}$ with $ku \pm a_i \in S$ (1), resp. $ku \pm a_i \in M$ (2), for $i = 1, \ldots, n$. Hence $kv \pm b = \sum_{i=1}^n (ku \pm a_i) x_i$ lies in M. □

For $(I, M \cap I)$ to have an order unit, it is obviously necessary that I is generated by elements of M. We see that this condition is already sufficient in many cases:

Corollary 5.2. *Let M be a pseudomodule over some archimedean semiring S in A. If I is any ideal in A generated by finitely many elements of M, then $(I, M \cap I)$ has an order unit.*

Proof. Indeed, this is 5.1(1). □

On the contrary, when M is merely an archimedean quadratic module in A, there do in general exist ideals I, generated by finitely many elements of M, such that $(I, M \cap I)$ does not have an order unit. We shall now construct such examples within a somewhat more general framework.

Proposition 5.3. *Assume $\frac{1}{2} \in A$. Let M be an archimedean quadratic module in A, and let I be a finitely generated ideal in A.*

(a) *$(I^2, M \cap I^2)$ always has an order unit.*
(b) *$(I, M \cap I)$ has an order unit if and only if $(I/I^2, \overline{M \cap I})$ has an order unit.*

For the proof we need the following easy observation:

Lemma 5.4. *Let G be an abelian group, $H \subset G$ a subgroup and $M \subset G$ a semigroup. If $(G/H, \overline{M})$ and $(H, M \cap H)$ both have order units, then (G, M) has an order unit.*

Proof. By assumption there exists $v \in M \cap H$ with $H \subset \mathbb{Z}v + M$, and there exists $u \in M$ with $G/H = \mathbb{Z}\bar{u} + \overline{M}$, i. e. $G = \mathbb{Z}u + M + H$. Hence $G = \mathbb{Z}u + \mathbb{Z}v + M$. From $-v = -(u+v) + u$ we get $\mathbb{Z}v \subset \mathbb{Z}(u+v) + M$, and similarly $\mathbb{Z}u \subset \mathbb{Z}(u+v) + M$. Therefore $G = \mathbb{Z}(u+v) + M$, which means that $u + v$ is an order unit of (G, M). □

Proof of 5.3. The ideal I^2 is generated by squares since $4ab = (a+b)^2 - (a-b)^2$. Hence (a) is a particular case of 5.1(2). Assertion (b) follows from (a) together with Lemma 5.4. □

Remarks 5.5.

1. In the situation of 5.3, assume that $I = (b_1, \ldots, b_m)$. Then $u := b_1^2 + \cdots + b_m^2$ is an order unit of $(I^2,\ M \cap I^2)$. Indeed, $u \pm b_i b_j$ is a sum of squares for all i, j, and so the $b_i b_j$ lie in $O(M,u)$. Since $O(M,u)$ is an ideal in A (3.2), and since the $b_i b_j$ generate I^2, we have $I^2 \subset O(M,u)$.

2. In 5.3(b), the quotient I/I^2 can be replaced by I/J for any ideal $J \subset I$ which is generated by finitely many sums of squares.

Here is a sample application.

Proposition 5.6. *Assume $\frac{1}{2} \in A$. Let $M = QM(g_1, \ldots, g_r, h_1, \ldots, h_m)$ be archimedean in A, and let $I = (g_1, \ldots, g_r)$. Assume that I is M-convex, $I = \sqrt{I}$, and that $h_1, \ldots, h_m$ are not zero divisors modulo I. Then $(I, M \cap I)$ has an order unit if and only if*

$$\big(I/I^2,\ \Sigma A^2 \cdot \bar{g}_1 + \cdots + \Sigma A^2 \cdot \bar{g}_r\big)$$

has an order unit.

Recall here that I is said to be M-convex if $I = \mathrm{supp}(M + I)$, or equivalently, if $a,\ b \in M$ and $a + b \in I$ imply $a,\ b \in I$. Yet another equivalent formulation is that $a,\ c \in I$, $b \in A$ and $a \leq_M b \leq_M c$ together imply $b \in I$. This last version explains why this property is called M-convexity.

Proof. This follows from Prop. 5.3(b) once we have shown

$$M \cap I \ \subset\ \Sigma A^2 \cdot g_1 + \cdots + \Sigma A^2 \cdot g_r + I^2.$$

To this end let $f \in M \cap I$, say

$$f = \sum_{i=1}^{r} s_i g_i + \sum_{j=0}^{m} t_j h_j$$

with $s_i,\ t_j \in \Sigma A^2$ und $h_0 := 1$. Then $\sum_{j=0}^{m} t_j h_j$ lies in I. This element is a sum of products $a^2 h_j$ with $a \in A$ and $j \in \{0, \ldots, m\}$. Since I is M-convex, all these $a^2 h_j$ lie in I. Moreover $a \in I$ in each case since $I = \sqrt{I}$ and the h_j are not zero divisors mod I. Therefore $\sum_j t_j h_j \in I^2$, which proves the proposition. □

Example 5.7. 1. In a geometric situation, e. g. for $A = \mathbb{R}[x_1, \ldots, x_n]$, the condition that I is M-convex is satisfied, for example, when I is the full vanishing ideal of a real algebraic set $V \subset \mathbb{R}^n$ for which $X(M) \cap V$ is Zariski-dense in V.

2. Let $A = \mathbb{R}[x, y]$ and $M = \mathrm{QM}(x, y, 1-x-y)$, an archimedean quadratic module in A. The ideal $I = (x)$ in A is generated by an element of M, but $(I, M \cap I)$ has no order unit.

Indeed, this is a particular case of Prop. 5.6: Via the identification $\mathbb{R}[y] \xrightarrow{\sim} I/I^2$, $g(y) \mapsto xg(y) + I^2$, the cone $\overline{M \cap I} = \Sigma\bar{x}$ in I/I^2 corresponds to the cone of sums of squares in $\mathbb{R}[y]$. Clearly, this cone does not have an order unit.

6. First applications

In this section we demonstrate how the approach via pure states gives a uniform and elegant approach to many (if not most) of the important known archimedean Stellensätze. Our proofs via pure states are shorter and more conceptual than the previously known proofs. In several cases we shall obtain versions that are considerably stronger than previously known.

The selection of applications presented here is not exhaustive. We plan to explain other applications elsewhere in a similar spirit.

Theorem 6.1 (Representation Theorem)**.** *Let M be a module over an archimedean semiring in A, and let $f \in A$ with $f > 0$ on $X(M)$. Then $nf \in M$ for some $n \in \mathbb{N}$.*

This fundamental theorem has been proved and re-discovered in many versions over the time, by Stone, Krivine, Kadison, Dubois and others (see, e. g., [Kr1], [Kr2]). See [PD], Sect. 5.6, for detailed historical remarks.

Proof. This is immediate from the criterion 2.5, since every pure state of $(A, M, 1)$ is an element of $X(M)$ by Corollary 4.4. □

The version for archimedean quadratic modules was proved by Putinar [Pu] in the geometric case, and by Jacobi [Ja] in an abstract setting. Again we get it easily using the approach via pure states:

Theorem 6.2. *Let M be an archimedean quadratic module in A, and let $f \in A$ with $f > 0$ on $X(M)$. Then $nf \in M$ for some $n \in \mathbb{N}$.*

Proof. The proof is the same as for Theorem 6.1, up to replacing the reference to Cor. 4.4 by a reference to Thm. 4.5. □

Remark 6.3. We just remind the reader that Theorems 6.1 and 6.2 have many celebrated applications. Among the best ones known are the Positivstellensätze by Schmüdgen [Sm] and by Putinar [Pu].

The following membership criterion, though more technical, played an important role in the proofs of various Nichtnegativstellensätze from the last years (see, e. g., [Sch4] Sect. 3, in particular 3.1.9):

Theorem 6.4. *Let M be an archimedean module over a semiring S in A, and assume that S is either archimedean or S is a preordering. Let $f \in A$ with $f \geq 0$ on $X(M)$. Suppose there is an identity $f = b_1 s_1 + \cdots + b_r s_r$ with $b_i \in A$ and $s_i \in S$ such that $b_i > 0$ on $Z(f) \cap X(M)$ $(i = 1, \ldots, r)$. Then $nf \in M$ for some $n \in \mathbb{N}$.*

The first version of Thm. 6.4 was given in [Sch1] Prop. 2.5. Later it was generalized substantially in [Sw2] Thm. 2. The statement of Thm. 6.4 above is still stronger than the version in [Sw2], at least essentially so, since the latter covered only the case $M = S$. (The slightly stronger conclusion $f \in S$, instead of $nf \in S$ for some $n \in \mathbb{N}$, was achieved in [Sw2] under the assumption $\frac{1}{q} \in S$ for some integer $q > 1$. It seems that this cannot be proved with the pure states method alone. Of course there is no difference when we assume $\mathbb{Q} \subset A$ and $\mathbb{Q}_+ \subset S$.)

Here is an easy proof of Thm. 6.4 using pure states:

Proof. Consider the ideal $I := (s_1, \ldots, s_r)$ in A. Then $u := s_1 + \cdots + s_r$ is an order unit of $(I, M \cap I)$ by Prop. 5.1 (2). Let φ be any pure state of $(I, M \cap I, u)$, and let $\phi\colon A \to \mathbb{R}$ be the associated ring homomorphism (4.12). Clearly $uM \subset M$, which implies $\phi \in X(M)$ (Cor. 4.12). We have $\varphi(s_i) \geq 0$ for $i = 1, \ldots, r$ and $\varphi(s_i) > 0$ for at least one i since $\sum_i \varphi(s_i) = 1$. By 2.5 it suffices to show $\varphi(f) > 0$.

First assume that φ is of type (I) (see 4.12), so $\varphi(f) = \frac{\phi(f)}{\phi(u)}$ with $\phi(u) \neq 0$. Note that $\phi \in X(M)$ implies $\phi(u) > 0$. Also, since $f \geq 0$ on $X(M)$, it implies $\phi(f) \geq 0$, whence $\varphi(f) \geq 0$. Assuming $\varphi(f) = 0$ would give $\phi \in Z(f) \cap X(M)$, hence $\phi(b_i) > 0$ $(i = 1, \ldots, r)$ by hypothesis. This would lead to a contradiction since $\varphi(f) = \sum_i \phi(b_i)\varphi(s_i)$. So $\varphi(f) > 0$ holds in case (I).

When φ is of type (II) then $\phi \in X(M+I) \subset X(M+Af) = Z(f) \cap X(M)$. So again $\phi(b_i) > 0$ for $i = 1, \ldots, r$, and $\varphi(f) = \sum_i \phi(b_i)\varphi(s_i)$ implies $\varphi(f) > 0$. □

In [Sch3] Thm 2.8, a local-global criterion was stated for membership in a module M over an archimedean preordering, in which the local conditions referred to the "localizations" of M with respect to the maximal ideals of A. This criterion has turned out to be quite powerful, cf. the applications mentioned in *loc. cit.*.

Using pure states it is easy to reprove this criterion, and in fact to strengthen it further:

Theorem 6.5. *Let S be an archimedean semiring and M an S-module in A. Let $f \in A$. For every maximal ideal $\mathfrak{m}$ of A, assume that there exists $s \in S$ with $s \notin \mathfrak{m}$ and $sf \in M$. Then $nf \in M$ for some $n \in \mathbb{N}$.*

Proof. Let $I := \operatorname{supp}(M + Af)$, and let J' be the ideal generated by $M \cap I$. For every maximal ideal $\mathfrak{m}$ of A there exists $s \in S$, $s \notin \mathfrak{m}$, with $sf \in M$, and hence $sf \in J'$. This shows $f \in J'$. (The argument is classical, we repeat it for the readers's convenience: Choose finitely many $s_i \in S$ with $(s_1, \ldots, s_r) = (1)$ and with $s_i f \in J'$ $(i = 1, \ldots, r)$, then multiply an equation $\sum_i a_i s_i = 1$ with f to see $f \in J'$.) Hence there are finitely many elements $x_1, \ldots, x_m \in M \cap I$ with $f \in (x_1, \ldots, x_m)$. Since $I = \operatorname{supp}(M + Af)$, there are $y_i \in M \cap I$ with $x_i + y_i \in Af$ $(i = 1, \ldots, r)$. Let $J :=$

$(x_1, \dots, x_r, y_1, \dots, y_r)$. Then $f \in J$, and $u := \sum_i (x_i + y_i)$ is an order unit of $(J, M \cap J)$ by 5.1(1). Note that $u = af$ for some $a \in A$.

Let φ be a pure state of $(J, M \cap J, u)$, we are going to show $\varphi(f) > 0$. Let ϕ be the associated ring homomorphism, so $\phi \in X(S)$ (Cor. 4.12). From $1 = \varphi(af) = \phi(a)\varphi(f)$ we get $\varphi(f) \neq 0$. On the other hand, there exists $s \in S$ with $\phi(s) \neq 0$ (hence $\phi(s) > 0$) and $sf \in M$. So $0 \leq \varphi(sf) = \phi(s)\varphi(f)$ shows $\varphi(f) \geq 0$. Altogether we get $\varphi(f) > 0$, and the proof is once more completed by an application of Theorem 2.5. □

Remark 6.6. When M is a quadratic module (so we can assume that S is a preordering), the local condition is needed only for the maximal ideals $\mathfrak{m} \supset \operatorname{supp}(M)$. (If there is $a \in \operatorname{supp}(M)$ with $a \notin \mathfrak{m}$, then $af \in \operatorname{supp}(M) \subset M$.) For such $\mathfrak{m}$, the condition simply says $f \in M_{\mathfrak{m}}$, where $M_{\mathfrak{m}}$ is the quadratic module generated by M in $A_{\mathfrak{m}}$.

When $\frac{1}{2} \in A$ and $M = S$ is a preordering, and if we assume $f \geq 0$ on $X(S)$, the local condition is only needed for $\mathfrak{m} \supset I = \operatorname{supp}(S + Af)$. (The brief argument is given in the proof of [Sch3] Cor. 2.10.)

7. More applications

We demonstrate now that the technique of pure states allows to establish archimedean Stellensätze that are completely new. Given a compact basic closed set $K \subset \mathbb{R}^n$ and a polynomial $f \in \mathbb{R}[\mathbf{x}]$ with $f|_K \geq 0$, all known results on denominator-free representations of f require (essentially) that the zero set of f in K is discrete, i. e., finite. In contrast, this zero set can be of arbitrary dimension in the two main results of this sections, Theorems 7.6 and 7.11 (see also Thm. 7.8).

Proposition 7.1. *Assume $\mathbb{Q} \subset A$. Let M be a module over an archimedean preordering S in A, let $f \in A$ with $f \geq 0$ on $X(M)$, and put $I := \operatorname{supp}(M + Af)$ (an ideal of A). Consider the following conditions:*

(i) *$f \in M$;*
(ii) *f lies in the ideal of A generated by $M \cap I$, and for every $\phi \in X(S+I)$ and every ϕ-linear map $\varphi\colon I \to \mathbb{R}$ with $\varphi|_{M\cap I} \geq 0$ one has $\varphi(f) \geq 0$.*

Then (ii) implies (i) if the ideal I is finitely generated. The converse (i) ⇒ (ii) holds unconditionally.

Remark: "$\varphi(f) \geq 0$" at the end of condition (ii) is not a misprint. However, (i) implies in fact $\varphi(f) > 0$ whenever φ is nonzero.

Proof. I is an ideal of A since $SI \subset I$ and $S + \mathbb{Z} = A$. The implication (i) ⇒ (ii) is trivial. We remark that $\varphi(f) > 0$ holds in (ii) whenever $\varphi \neq 0$. Indeed, f is an order unit of $(I, M \cap I)$ according to Cor. 3.6.

Conversely assume that (ii) holds and I is finitely generated. Let J be the ideal generated by $M \cap I$. Since $I = (M \cap I) + Af$, it is clear that $I = J + Af$. So $f \in J$ implies $J = I$. Choose generators $x_1, \dots, x_r \in M$ of I. There are elements $y_i \in M \cap I$ with $x_i + y_i \in Af$ $(i = 1, \dots, r)$.

The element $u := \sum_i (x_i + y_i)$ lies in Af, and is an order unit of $(I, M \cap I)$ by 5.1. Applying 2.5, we have to show $\varphi(f) > 0$ for every pure state φ of $(I, M \cap I, u)$.

Given such φ, let $\phi \in X(S)$ be the associated ring homomorphism (Cor. 4.12). From $u \in Af$ we see that $\varphi(f) \neq 0$. If φ is of type (II) then $\varphi(f) \geq 0$ by the hypothesis. Assume that φ is of type (I), i. e., $\phi(u) \neq 0$. From $u^2 \in M \cap I$ and $\varphi(u^2) = \phi(u)$ we see $\phi(u) > 0$. For any $x \in M$ we have $u^2 x \in M \cap I$, therefore $0 \leq \varphi(u^2 x) = \phi(u)\phi(x)$, which implies $\phi(x) \geq 0$. Hence $\phi \in X(M)$, and so $\phi(f) \geq 0$ follows from the hypothesis. □

Remark 7.2. At first sight it is surprising that $\varphi(f) \geq 0$ in (ii) should suffice (instead of $\varphi(f) > 0$). The subtlety, however, lies in the ideal I and in the condition that f should lie in the ideal generated by $M \cap I$. In concrete situations it is often hard to decide whether this is true. Even when S is a preordering in $\mathbb{R}[x_1, \ldots, x_n]$ given by finitely many explicit generators, there seems no general procedure known to produce generators for the support ideal $\mathrm{supp}(S)$. For these reasons, Prop. 7.1 seems to be mainly of theoretical interest.

Proposition 7.3. *Let A be an $\mathbb{R}$-algebra, let $S \subset A$ be a semiring and $M \subset A$ an archimedean S-module. Assume that S is either archimedean or a preordering. Let $f \in A$ with $f \geq 0$ on $X(M)$. Assume there are $g_1, \ldots, g_r \in S$ that vanish identically on $Z(f) \cap X(M)$, such that the following two conditions are satisfied:*

(1) *$f \in I := (g_1, \ldots, g_r)$;*
(2) *for every $\phi \in Z(f) \cap X(M)$, the residue class $\bar{f}$ lies in the interior of the cone $\mathbb{R}_+ \bar{g}_1 + \cdots + \mathbb{R}_+ \bar{g}_r \subset I/\mathfrak{m}_\phi I$, where $\mathfrak{m}_\phi := \ker(\phi)$.*

Then $f \in M$.

Note that $I/\mathfrak{m}_\phi I$ is an $\mathbb{R}$-vector space of finite dimension, which explains the meaning of interior in (2). It is clear how to give a dual formulation of (2) using states.

Proof. By Prop. 5.1(2), $u := g_1 + \cdots + g_r$ is an order unit of $(I, M \cap I)$. Note $u \in S$. Let $\varphi\colon I \to \mathbb{R}$ be a pure state of $(I, M \cap I, u)$. We shall show $\varphi(f) > 0$, which implies $f \in M$ by Thm. 2.5. Let $\phi \in X(S)$ be the ring homomorphism associated to φ. For every $x \in M$ we have $xu \in M \cap I$, and so $0 \leq \varphi(xu) = \phi(x)$. This shows $\phi \in X(M)$, and so $\phi(f) \geq 0$ by hypothesis. Moreover, there are two possibilities (Cor. 4.12):

1. If φ is of type (I) then $\phi(u) \neq 0$, and hence $\phi(u) > 0$ since $u \in S$. Assuming $\phi(f) = 0$ would mean $\phi \in Z(f) \cap X(M)$. This would imply $\phi(g_i) = 0$ for all i, contradicting $\phi(u) > 0$. So $\phi(f) > 0$, and hence $\varphi(f) = \frac{\phi(f)}{\phi(u)} > 0$.

2. If φ is of type (II) then $\phi \in Z(f) \cap X(M)$. The map φ is induced by a ϕ-linear map $\bar{\varphi}\colon I/\mathfrak{m}_\phi I \to \mathbb{R}$ satisfying $\bar{\varphi}(\overline{M \cap I}) \geq 0$. In particular, $\bar{\varphi} \geq 0$ on the cone $\mathbb{R}_+ g_1 + \cdots + \mathbb{R}_+ g_r$. Since $\bar{f}$ lies in the interior of this cone by assumption (2), we again get $\varphi(f) = \bar{\varphi}(\bar{f}) > 0$. □

Remarks 7.4.

1. Given $g_1, \dots, g_r \in S$ that vanish on $Z(f) \cap X(M)$, conditions (1) and (2) in Prop. 7.3 can be effectively checked, for example when A is a polynomial ring over $\mathbb{R}$.

2. In Prop. 7.3, assume that S is an archimedean semiring and $M = S$. Then the sufficient conditions of 7.3 are also necessary for $f \in S$, in the sense that $f \in S$ implies the existence of $g_1, \dots, g_r \in S$ satisfying (1) and (2). (One can simply take $r = 1$ and $g_1 = f$.)

3. Assume we are given S, M and f as in 7.3, with $f \geq 0$ on $X(M)$, and we want to prove $f \in M$ using this theorem. In general, it is a subtle task to find a suitable ideal I as in this theorem (together with its generators), since conditions (1) and (2) tend to work against each other: (1) asks for I being large, (2) asks for I being small.

Using the abstract criteria established so far, we shall now obtain applications in geometric situations that are more concrete. In doing so, the question arises how interpret conditions like 7.3(2) in a geometric way. Under suitable regularity assumptions, this turns out to be possible.

First, we need the following lemma:

Lemma 7.5. *Let $(A, \mathfrak{m})$ be a regular local ring, and let $I \neq (1)$ be an ideal. If A/I is regular then for any $n \geq 1$ the map*

$$I^n/\mathfrak{m}I^n \to \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

induced by $I^n \subset \mathfrak{m}^n$ is injective. Conversely, if this map is injective for $n = 1$, then A/I is regular.

Proof. Injectivity of this map for $n = 1$ means that I can be generated by a subsequence $(x_1, \dots, x_d)$ of a regular parameter system of $(A, \mathfrak{m})$. It is well known that this is equivalent to A/I being regular (e. g., [Mt] Thm. 14.2). Assuming that this is the case, the ideal I^n is generated by the monomials $x^\alpha = x_1^{\alpha_1} \cdots x_d^{\alpha_d}$ of degree $|\alpha| = n$. These are linearly independent in $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ over $A/\mathfrak{m}$ (*loc. cit.*, Thm. 14.4), and so the map $I^n/\mathfrak{m}I^n \to \mathfrak{m}^n/\mathfrak{m}^{n+1}$ is injective as well. □

Here is an application of Prop. 7.3 to a geometric situation. We write $\mathbb{R}[\mathtt{x}] := \mathbb{R}[x_1, \dots, x_n]$.

Theorem 7.6. *Let $S \subset \mathbb{R}[\mathtt{x}]$ be a semiring and M an archimedean S-module. Assume that S is either archimedean or a preordering. Let $f \in \mathbb{R}[\mathtt{x}]$ with $f \geq 0$ on $X(M)$, and let V be the (reduced) Zariski closure of $Z(f) \cap X(M) \subset \mathbb{R}^n$ in $\mathbb{A}^n$. Assume there are $g_1, \dots, g_r \in S$ vanishing on $Z(f) \cap X(M)$ with*

(1) *$f \in (g_1, \dots, g_r)$;*
(2) *for every $z \in Z(f) \cap X(M)$ and every $v \in \mathbb{R}^n$ with $D_v g_i(z) \geq 0$ $(i = 1, \dots, r)$ and $v \notin T_z(V)$ we have $D_v f(z) > 0$.*

If moreover every point $z \in Z(f) \cap X(M)$ is a nonsingular point of V, then $f \in M$.

Here we have written $D_v f(z)$ for the directional derivative of f at z in the direction v, i. e.,

$$D_v f(z) \;=\; \lim_{t \to 0} \frac{f(z+tv) - f(z)}{t}.$$

Proof. Write $A := \mathbb{R}[\mathbf{x}]$ and $I := (g_1, \ldots, g_r)$, and let J be the vanishing ideal of V in A. We are going to apply Prop. 7.3. To verify hypothesis (2) there, fix $z \in Z(f) \cap X(M)$, and let $\mathfrak{m} := \mathfrak{m}_z$ be the corresponding maximal ideal of A. Note that $I \subset J \subset \mathfrak{m}$.

We first show $I + \mathfrak{m}^2 = J + \mathfrak{m}^2$. Assume to the contrary that the inclusion $I + \mathfrak{m}^2 \subset J + \mathfrak{m}^2$ is strict. Then there exists a linear form $\psi \in (\mathfrak{m}/\mathfrak{m}^2)^\vee$ vanishing on all residue classes of elements of I, but not on all residue classes of elements of J. This means that there is a vector $v \in \mathbb{R}^n$ with $v \notin T_z(V)$ and with $D_v g(z) = 0$ for all $g \in I$. But this contradicts assumption (2), since we cannot have $D_{\pm v} f(z) > 0$ for both signs $\pm$.

Next we show that the elements of $(I/\mathfrak{m}I)^\vee$ are directional derivatives at z. It is enough to prove that the map $I/\mathfrak{m}I \to \mathfrak{m}/\mathfrak{m}^2$ induced by the inclusion $I \subset \mathfrak{m}$ is injective. Since $A_\mathfrak{m}/JA_\mathfrak{m}$ is a regular local ring by hypothesis, the map $J/\mathfrak{m}J \to \mathfrak{m}/\mathfrak{m}^2$ is injective (Lemma 7.5), which means $J \cap \mathfrak{m}^2 = \mathfrak{m}J$. On the other hand, $I + (J \cap \mathfrak{m}^2) = J$ by what has just been proven. So $I + \mathfrak{m}J = J$. By the Nakayama lemma this implies $IA_\mathfrak{m} = JA_\mathfrak{m}$, and so $I/\mathfrak{m}I \to \mathfrak{m}/\mathfrak{m}^2$ is injective as desired.

Therefore, when v runs through the vectors in $\mathbb{R}^n$ as in (2), then $\varphi_v \colon \bar{g} \mapsto D_v g(z)$ ($\bar{g} \in I/\mathfrak{m}I$) runs through the nonzero elements in the dual of the cone $\mathbb{R}_+\bar{g}_1 + \cdots + \mathbb{R}_+\bar{g}_r \subset I/\mathfrak{m}I$. So we see that condition (2) in 7.6 corresponds precisely to (2) in Prop. 7.3. The proof is therefore complete. □

Remarks 7.7.

1. For Thm. 7.6, it is not necessary to work in a polynomial ring $\mathbb{R}[\mathbf{x}]$, resp. in affine space $\mathbb{A}^n$. One could replace $\mathbb{A}^n$ by any nonsingular affine $\mathbb{R}$-variety, if one is willing to reformulate condition (2) properly in this setting. We restricted to the case of the polynomial ring only to allow a less technical formulation.

2. Let W be the Zariski closure of $X(M)$. Then the hypotheses of Theorem 7.6 imply that every point $z \in Z(f) \cap X(M)$ is a boundary point of $X(M)$ relative to $W(\mathbb{R})$, except when f vanishes identically on a neighborhood of z in $X(M)$. Indeed, otherwise $T_z(V) \subsetneqq T_z(W)$, and there would be a neighborhood of z in $W(\mathbb{R})$ on which $g_1, \ldots, g_r$ are nonnegative. Choose any $v \in T_z(W)$ with $v \notin T_z(V)$ and apply (2) to $\pm v$ to get a contradiction. (By $T_z(W)$ we denote the tangent space of W at z in $\mathbb{R}^n$.)

Here is a particularly concrete case of Thm. 7.6. Again we denote $\mathbb{R}[\mathbf{x}] = \mathbb{R}[x_1, \ldots, x_n]$.

Theorem 7.8. *Let $K \subset \mathbb{R}^n$ be a nonempty compact convex polyhedron, described by linear inequalities $g_1 \geq 0, \ldots, g_s \geq 0$. Let S be the semiring in $\mathbb{R}[\mathbf{x}]$ generated by $\mathbb{R}_+$ and $g_1, \ldots, g_s$. Let F be a face of K, and let $f \in \mathbb{R}[\mathbf{x}]$ satisfy $f|_F = 0$ and $f|_{K \setminus F} > 0$. For every $z \in F$ and every $y \in K \setminus F$ assume $D_{y-z} f(z) > 0$. Then $f \in S$.*

Speaking informally, the last hypothesis says that every directional derivative of f at a point of F pointing into K and not tangential to F should be strictly positive.

Proof. By Remark 3.3, S is archimedean. After relabelling the g_i we can assume that $g_1, \ldots, g_r$ vanish identically on F while $g_{r+1}, \ldots, g_s$ don't, where $1 \leq r \leq s$. Then $I := (g_1, \ldots, g_r)$ is the full vanishing ideal of the affine subspace V spanned by F, and so $f \in I$.

We are going to apply Theorem 7.6 with $M = S$. Condition (1) has just been established. In view of (2) fix $z \in F$, and let $v \in \mathbb{R}^n$ with $v \notin T_z(V)$ and $D_v g_i(z) \geq 0$ for $i = 1, \ldots, r$. We need to show $D_v f(z) > 0$.

For this we would like to assure that $z + bv \in K$ for small $b > 0$. A priori, this need not be the case. However, we still have some freedom to adjust v. Choose $w \in \mathbb{R}^n$ such that $z + \varepsilon w$ lies in the relative interior of F for small $\varepsilon > 0$. Then for every index $j \in \{r+1, \ldots, s\}$ we have either $g_j(z) > 0$ or $D_w g_j(z) > 0$. Replace v by $v + tw$ for large $t > 0$. This doesn't change $D_v a(z)$ for $a \in I$, but in this way we can achieve $D_v g_j(z) > 0$ for every $j \in \{1, \ldots, s\}$ with $g_j(z) = 0$. Therefore, $z + bv \in K \setminus F$ for small $b > 0$, which means $v = c(y - z)$ for suitable $c > 0$ and $y \in K \setminus F$. From the hypothesis made on f we therefore conclude $D_v f(z) > 0$. □

Remark 7.9. In the situation of Theorem 7.8, it was so far not even known whether f would lie in the preordering $\mathrm{PO}(g_1, \ldots, g_r)$ except when F is a face of codimension one. (In this case, after extracting from f the linear equation for F with the maximal possible power, one is left with a polynomial which is strictly positive on K.)

Example 7.10. Consider the simplex

$$K \;=\; \Big\{ x \in \mathbb{R}^n \colon x_1 \geq 0, \ldots, x_n \geq 0, \; \sum_{i=1}^{n} x_i \leq 1 \Big\}$$

in $\mathbb{R}^n$, and let $S \subset \mathbb{R}[x_1, \ldots, x_n]$ be the semiring generated by $\mathbb{R}_+$ and $x_1, \ldots, x_n$, $1 - \sum_{i=1}^n x_i$. Consider the face $F = K \cap \{x_1 = \cdots = x_r = 0\}$ of K (with $1 \leq r \leq n$ being fixed). Given a polynomial f with $f > 0$ on $K \setminus F$ and $f = 0$ on F, we have $f \in S$ provided that $\partial_{x_1} f, \ldots, \partial_{x_r} f$ are strictly positive on F.

While Theorem 7.6 applies only in cases where the zeros of f in $X(M)$ lie on the boundary of $X(M)$ (see Remark 7.7), we will now mention a result which applies when f vanishes in interior points of $X(M)$.

Theorem 7.11. *Let $M = QM(g_1, \ldots, g_m)$ be an archimedean quadratic module in $\mathbb{R}[\mathbf{x}]$. Let $f \in \mathbb{R}[\mathbf{x}]$ with $f \geq 0$ on $X(M)$. Assume that the (reduced) Zariski closure V of $Z(f) \cap X(M)$ in $\mathbb{A}^n$ is a local complete intersection. For every point $z \in Z(f) \cap X(M)$, assume moreover:*

(1) *z is a nonsingular point of V,*
(2) *$\nabla f(z) = 0$,*
(3) *$D^2 f(z)[v, v] > 0$ for all $v \in \mathbb{R}^n$ with $v \notin T_z(V)$.*

Then $f \in M$.

Here $D^2 f(p)[v, w]$ denotes the evaluation of the Hessian $D^2 f(p)$ at the pair of vectors (v, w).

Proof. Let J be the vanishing ideal of V in $\mathbb{R}[\mathbf{x}]$. We have $f \in J$ and are going to show $f \in J^2$. First fix $z \in Z(f) \cap X(M)$, let $\mathfrak{m} = \mathfrak{m}_z$ be the corresponding maximal ideal of $\mathbb{R}[\mathbf{x}]$. Then $f \in \mathfrak{m}^2$ since $\nabla f(z) = 0$. Since V is a local complete intersection, J/J^2 is locally free as a module over $\mathbb{R}[V] = \mathbb{R}[\mathbf{x}]/J$ (e. g. [H], pp. 184–185). Since $\bar{f} \in \mathfrak{m}_z J/J^2$ for every $z \in Z(f) \cap X(M)$, and since this set is Zariski dense in V, it follows that $f \in J^2$.

By Prop. 5.3(a), $(J^2, M \cap J^2)$ has an order unit u. Let φ be a pure state of $(J^2, M \cap J^2, u)$, we shall show $\varphi(f) > 0$. If φ is of type (I) then, up to positive scaling, φ is evaluation in some point of $X(M)$ outside $Z(f)$, and so $\varphi(f) > 0$. If φ is of type (II), there is a point $z \in Z(f) \cap X(M)$ such that φ is induced by a linear map $\bar{\varphi}\colon J^2/\mathfrak{m}J^2 \to \mathbb{R}$, where $\mathfrak{m} := \mathfrak{m}_z$. Since z is a nonsingular point of V, the map $J^2/\mathfrak{m}J^2 \to \mathfrak{m}^2/\mathfrak{m}^3$ induced by the inclusion $J^2 \subset \mathfrak{m}^2$ is injective (Lemma 7.5). The inclusion $J/\mathfrak{m}J \hookrightarrow \mathfrak{m}/\mathfrak{m}^2$ induces an inclusion of the second symmetric powers of these vector spaces, which is $J^2/\mathfrak{m}J^2 \hookrightarrow \mathfrak{m}^2/\mathfrak{m}^3$. The linear map $\bar{\varphi}$ can therefore be seen as a positive semidefinite symmetric bilinear form on $J/\mathfrak{m}J$. As such it can be extended to $\mathfrak{m}/\mathfrak{m}^2$. This yields a linear extension $\tilde{\varphi} \in (\mathfrak{m}^2/\mathfrak{m}^3)^\vee$ of $\bar{\varphi}$ such that $\tilde{\varphi}(\bar{g}^2) \geq 0$ for all $g \in \mathfrak{m}$. Since the elements of $(\mathfrak{m}^2/\mathfrak{m}^3)^\vee$ are the symmetric second order differential operators at z, it follows that there is a positive semidefinite symmetric matrix (s_{ij}) such that $\varphi(g) = \sum_{i,j} s_{ij} \partial_{x_i} \partial_{x_j} g(z)$ for all $g \in J^2$. In particular, there are vectors $v_1, \ldots, v_k$ in $\mathbb{R}^n$ with

$$\varphi(g) = \sum_{i=1}^{k} D^2 g(z)[v_i, v_i]$$

for every $g \in J^2$. Since φ does not vanish identically on J^2 we have $v_i \notin T_p(V)$ for at least one index i. Therefore $\varphi(f) > 0$ follows from the hypothesis. □

Remark 7.12. The condition in Thm. 7.11 that V is a local complete intersection means that the ideal J of V in $\mathbb{R}[\mathbf{x}]$ can locally be generated by $n - \dim(V)$ many elements. It is satisfied if V is nonsingular, but the condition is much more general.

Example 7.13. We illustrate the use of Thm. 7.11 by an example. Let M be an archimedean quadratic module in $\mathbb{R}[x, y, z]$, let $K = X(M)$, and let $Z = \{(0, 0, t) \colon t \in \mathbb{R}\}$ be the z-axis in $\mathbb{R}^3$. Assume that p, q, $r \in \mathbb{R}[x, y, z]$ are such that

$$f \;=\; x^2 \cdot p + y^2 \cdot q + 2xy \cdot r$$

satisfies $f > 0$ on $K \setminus Z$ and $f = 0$ on Z. Then $f \in M$, provided that p and $pq - r^2$ are strictly positive on $Z \cap K$. This follows by a direct application of 7.11.

Acknowledgments

We are indebted to David Handelman for pointing out to us the relevance of pure states on ideals to certificates of nonnegativity. At the very early stages of this work, the third author appreciated many stimulating discussions with Daniel Plaumann.

References

[Ba] A. Barvinok: *A Course in Convexity*. Grad. Stud. Math. **54**, AMS, Providence, RI, 2002.

[BLP] F. Bonsall, J. Lindenstrauss, R. Phelps: Extreme positive operators on algebras of functions. *Math. Scand.* **18**, 161–182 (1966).

[EHS] E. Effros, D. Handelman, C. L. Shen: Dimension groups and their affine representations. *Am. J. Math.* **102**, 385–407 (1980).

[Ei] M. Eidelheit: Zur Theorie der konvexen Mengen in linearen normierten Räumen. *Stud. Math.* **6**, 104–111 (1936).

[Go] K. R. Goodearl: *Partially Ordered Abelian Groups with Interpolation*. Math. Surv. Monographs **20**, AMS, Providence, RI, 1986.

[GH] K. R. Goodearl, D. Handelman: Rank functions and K_0 of regular rings. *J. Pure Appl. Algebra* **7**, 195–216 (1976).

[H1] D. Handelman: *Positive Polynomials and Product Type Actions of Compact Groups*. Mem. Am. Math. Soc. **54**, Providence, RI, 1985.

[H2] ———: Polynomials with a positive power. *Contemp. Math.* **135**, AMS, Providence, RI, 229–230 (1992).

[H] R. Hartshorne: *Algebraic Geometry*. Grad. Texts Math. **52**, Springer, New York, 1977.

[Ja] Th. Jacobi: A representation theorem for certain partially ordered commutative rings. *Math. Z.* **237**, 259–273 (2001).

[JP] Th. Jacobi, A. Prestel: Distinguished representations of strictly positive polynomials. *J. reine angew. Math.* **532**, 223–235 (2001).

[Kk] S. Kakutani: Ein Beweis des Satzes von M. Eidelheit über konvexe Mengen. *Proc. Imp. Acad. Tokyo* **13**, 93–94 (1937).

[Kö] G. Köthe: *Topological Vector Spaces I*. Grundl. math. Wiss. **159**, Springer, Berlin, 1969.

[Kr1] J.-L. Krivine: Anneaux préordonnés. *J. Analyse Math.* **12**, 307–326 (1964).

[Kr2] ———: Quelques propriétés des préordres dans les anneaux commutatifs unitaires. *C. R. Acad. Sci. Paris* **258**, 3417–3418 (1964).

[La] M. Laurent: Sums of squares, moment matrices and optimization over polynomials. In: *Emerging Applications of Algebraic Geometry*, (M. Putinar, S. Sullivant, eds.), IMA Volumes Math. Appl. **149**, Springer, New York, 2009, pp. 157–270.

[Ma1] M. Marshall: Representation of non-negative polynomials with finitely many zeros. *Ann. Fac. Sci. Toulouse* (6) **15**, 599–609 (2006).

[Ma2] M. Marshall: *Positive Polynomials and Sums of Squares*. Math. Surv. Monographs **146**, AMS, Providence, RI, 2008.

[Mt] H. Matsumura: *Commutative Ring Theory*. Cambridge Univ. Press, Cambridge, 1986.

[PD] A. Prestel, Ch. Delzell: *Positive Polynomials*. Monographs Math., Springer, Berlin, 2001.

[Pu] M. Putinar: Positive polynomials on compact semi-algebraic sets. *Indiana Univ. Math. J.* **42**, 969–984 (1993).

[Sch1] C. Scheiderer: Sums of squares on real algebraic curves. *Math. Z.* **245**, 725–760 (2003).

[Sch2] ———: Distinguished representations of non-negative polynomials. *J. Algebra* **289**, 558–573 (2005).

[Sch3] ———: Sums of squares on real algebraic surfaces. *Manuscr. math.* **119**, 395–410 (2006).

[Sch4] ———: Positivity and sums of squares: A guide to recent results. In: *Emerging Applications of Algebraic Geometry*, (M. Putinar, S. Sullivant, eds.), IMA Volumes Math. Appl. **149**, Springer, New York, 2009, pp. 271–324.

[Sm] K. Schmüdgen: The K-moment problem for compact semi-algebraic sets. *Math. Ann.* **289**, 203–206 (1991).

[Sw1] M. Schweighofer: Iterated rings of bounded elements and generalizations of Schmüdgen's Positivstellensatz. *J. reine angew. Math.* **554**, 19–45 (2003).

[Sw2] ———: Certificates for nonnegativity of polynomials with zeros on compact semi-algebraic sets. *Manuscr. math.* **117**, 407–428 (2005).

[St] G. Stengle: A nullstellensatz and a positivstellensatz in semialgebraic geometry. *Math. Ann.* **207**, 87–97 (1974).

Institut de Recherche Mathématique de Rennes, Université de Rennes I, Campus de Beaulieu, 35042 Rennes cedex, France

E-mail address: sabine.burgdorf@univ-rennes1.fr

Universität Konstanz, Fachbereich Mathematik und Statistik, 78457 Konstanz, Allemagne

E-mail address: claus.scheiderer@uni-konstanz.de

Institut de Recherche Mathématique de Rennes, Université de Rennes I, Campus de Beaulieu, 35042 Rennes cedex, France

E-mail address: markus.schweighofer@univ-rennes1.fr